

Failover

Key Benefits

- Ensure maximum system up time and peace of mind
- Get continuous access to live video streams always
- Use powerful archiving mechanisms to secure video recordings
- Complement Failover features with edge recording and off-the-shelf solutions



Achieve Uninterrupted System Access and Data Protection

When you have critical assets to protect, it is important to rely on a security system that provides continuous access and that can tolerate hardware failures without any system interruption. [Security Center](#) provides multiple mechanisms to ensure the system is up at all times and critical information is always available. Security Center's role-based architecture ensures Failover by allowing each role to be powered by multiple servers, reducing the risk of a single point of failure.

Get Built-in Failover Directory and Load Balancing

The Directory Role is responsible for handling client connections and enforcing security policies, making most of the decisions in the system, handling workflows, and storing the system configuration. The Failover Directory solution built-in the Security Center can provide hot standby and load balancing simultaneously, protecting up to five failover directories at once. Therefore, you no longer have to worry about which Directory to connect to; the system will automatically connect to the least busy Directory.

To simplify the user experience, Security Center also offers two mechanisms for database synchronization: backup and restore mode, and SQL Mirroring mode. The backup and restore mode consists of transferring the primary database to the Failover Directory servers at a pre-defined interval, and the SQL Mirroring mode offers continuous synchronization.

Ensure Uninterrupted Video Streaming

In the eventuality that all Directories become unavailable, you will lose connection to the system and thus will not have the ability to execute new actions and commands. In this degraded mode, the Uninterrupted Video Streaming feature of Security Center will preserve access to live video streaming so you can keep an eye on the cameras even if the system is partially interrupted.

Minimize Video Recording Loss with Failover and Redundant Archiving

Failover and Redundant Archiving helps you protect video recordings from hardware and software failures as well as storage failures and network interruptions. Similar to the other roles, the Security Center Archiver has the ability to be powered by another server, and the additional server being designated as the standby Archiver. To minimize video recording loss, the standby Archiver is already connected to the cameras which ensure that recording and live streaming is recovered in a matter of seconds. To completely eliminate any loss of recording, redundant Archiving can be activated so that the standby Archiver also records the cameras on the same schedule.

Save Bandwidth with Auxiliary Archiving

The Auxiliary Archiver has the ability to record a different stream from the camera than the archiver leveraging the multi-streaming capabilities of the cameras. This allows the Auxiliary Archiver to record, for example, a higher quality stream for a short retention period. In investigations, you can access short-term high-quality video without having to spend a lot of money on storage. And since the Auxiliary Archiver simply receives the stream from the cameras, it can be installed on a different network than the cameras or in a completely separate building, town or country providing off-site recording of a lower quality stream in order not to overload the WAN.

Back-Up Video Recordings using Edge Recording

By leveraging edge recording capabilities (e.g., SD cards, NAS) of certain cameras, you can eliminate continuous streaming to a central archiver. For additional protection, downloads of the recorded video on the cameras can be scheduled and transferred back to a central archiver at any point and time using Genetec's [Video Trickling feature](#).

Strengthen Fault Tolerance with Off-the-Shelf Solutions

Genetec is cognizant that there is not always a single solution that fits all. Therefore, in order to support existing IT practices and procedures in some organizations, Security Center is also fully compatible with the most common off-the-shelf solutions for system protection. In fact, Security Center supports Windows and NEC clustering solutions and can be deployed in virtual environments such as VMware® ESX/ESXi.